SVD and Lifting Wavelet Based Fragile Image Watermarking

Swanirbhar Majumder[1], Tirtha Sankar Das[2], Souvik Sarkar[2], and Subir Kumar Sarkar[2]
[1] Department of ECE, NERIST (Deemed University), Arunachal Pradesh 791109, India
Email: swanirbhar@gmail.com
[2] Department of ETCE, Jadavpur University,Kolkata, West Bengal, India
Email: tirthasankardas@yahoo.com, sksarkar@etce.jdvu.ac.in

***Abstract*—Creation and distribution of digital multimedia, by copying and editing, has both advantages and disadvantages. These can facilitate unauthorized usage, misappropriation, and misrepresentation. Therefore the content providers have become more concerned. So image watermarking, which is the act of embedding another signal (the watermark) into an image, have been proposed for copyright protection and authentication by robust and fragile methodologies respectively. So for various applications, there are different watermarking algorithms, but here this work is mainly for authentication as the watermarking scheme is fragile. The discrete lifting based wavelet transform and the singular value decomposition (SVD) algorithms are used in this scheme. The former for the carrier or the image to be authenticated, while the latter for the logo which is embedded in the carrier. The distribution of SVD compressed pixel values are distributed in the wavelet domain based on a pseudorandom sequence. This has been observed to test the integrity of the stego image and its authentication. Moreover due to usage of lifting based wavelet transform and SVD the hardware implementability is better.**

***Index Terms*—Fragile watermarking, SVD, Lifting based wavelet transform, pseudorandom sequence, stego image.**

I. INTRODUCTION

With the advances in digital media, and easier distribution of multimedia data like images, songs, videos, or any other type of data, along with advancement of software applications has become a boon as well as a curse to the whole world. At one end it is a necessity while on other thoughts, unauthorized usage, misappropriation, and misrepresentation are its drawbacks. Thus we go for copyright protection and authentication of all multimedia data to be at the safer side, and avoid cyber criminals.

One of the popular ways of doing it is watermarking, which may be robust or fragile. Here a fragile watermarking scheme is presented. All popular fragile image watermarking schemes are used for image authentication and verification of data integrity [1]. Due to this, applications like lossy compression are not tolerated in image transmission or storage as the fragile watermarks are destroyed [2] [3]. This is normally done by embedding patterns imperceptibly in the least significant bit (LSB) or as hash values [4] [5].

But to classify outwardly there are mainly two types of fragile watermarking, one done spatially [5] [6] [7] and the other in the transform domain [2] [8] [9]. To be regarded as a good image authenticating watermarking scheme the fragile watermark should necessarily fulfill some conditions. For the scheme of fragile watermark presented here mainly two transforms are used one for the carrier image, and the other for the logo or watermark to be embedded in the carrier. Lifting based wavelet transform with spline 5/3 wavelet has been used for the carrier image and singular value decomposition based image compression scheme has been used for the logo or watermark.

A. Lifting Based Wavelet Transform

Instead of the traditional DWT method multi-level discrete two-dimension wavelet transform based on lifting method is used. It is multilevel as based on algorithm the level can be decided on. The wavelets used are Cohen-Daubechies-Feauveau (CDF) 9/7 wavelet, which is the name 'cdf97' and spline 5/3 with the name 'spl53', specifically. Still other wavelets can be used as well as per the necessity of the watermarking application. Here step wise 1-D FWT is performed based on lifting method to get the whole set of multilevel transform. This is actually a deliberately organized lifting structure provided as an intermediate block of the multilevel wavelet transform.

The lifting structure is organized such that a 1-by-1 structure with two field lambda (λ_z) and two-element lifting gain vectors are used. Therefore first a lazy wavelet [10] is incorporated with alternated lifting (LF) and dual lifting (DLF) steps for lambda (λ_z) being a 1-by-M structure if M lifting units as in figure 2 based on the Laurent polynomials. Here there are two lambda (λ_z) fields for coefficients and order which denote the transfer function of every lifting unit. The final stage has the scaling functions to rescale the output. Thus for a wavelet transform with 3 lifting units as under:

$$\lambda_1 = a_1 + a_2 z \,;\, \lambda_2 = b_1 + b_2 z^{-1} ; \lambda_3 = c_1 z^{-1} + c_2 z \quad (1)$$

Thus the data structure of lambda (λ_z) will be composed of the coefficients and order or z:

$$\lambda_z = struct\left(\begin{bmatrix} a_1 & a_2 \\ b_1 & b_2 \\ c_1 & c_2 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & -1 \\ -1 & 1 \end{bmatrix} \right) \quad (2)$$

This structure of lambda (λ_z) is again under another structure for the final scaling based on itself and the two

DOI: 01.IJSIP.02.01.83

element lifting gains [K0=1/K, K1=K] to produce the 1-by-1 structure with two fields lambda (λ_z) and scaling factor K of the structure denoted by L.

$$L = struct(\lambda_z, [K_0, K_1]) \tag{3}$$

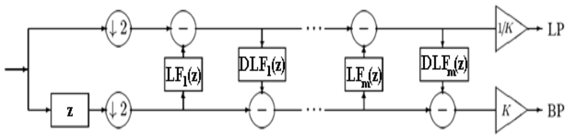

Figure 1. The forward wavelet transform with lazy wavelet, alternating lifting and dual lifting and scaling at the end.

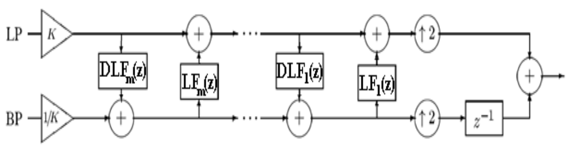

Figure 2. The inverse wavelet transform with scaling, alternating lifting and dual lifting and inverse lazy wavelet at the end.

The inverse transform can immediately be derived from the forward by running the scheme backwards as in figure 2. Here there is first a scaling, then alternating dual lifting and lifting steps, and finally the inverse Lazy transform.

B. Singular Value Decomposition

Singular value decomposition (SVD) technique, a generalization of the eigen-value decomposition, is used to analyze rectangular matrices and has been used in many areas of image processing as well. The main idea of the SVD is to decompose a rectangular matrix into three simple matrices (two orthogonal matrices and one diagonal matrix) [11] [12]. It has been widely studied and used for watermarking by researchers for long. But unlike the other schemes here it has been used to compress the logo to be watermarked. Thereby utilizing the image compression scheme of SVD here, and not for watermarking [13-17]. Moreover the orthogonal matrices and the diagonal matrix are embedded in the carrier instead of the logo image itself.

II. The Watermarking Scheme

A. Watermark Embeddeding Process

The carrier image, which here is the standard 'lena' image firstly, is undergone 3 level lifting based two dimensional discrete wavelet transform using the spline 5/3, 'spl53' wavelet. On this wavelet domain image which has sub bands LL3, LH3, HL3, HH3, LH2, HL2, HH2, LH1, HL1 and HH1. Here LL stands for the approximate coefficients, LH for the horizontal coefficients, HL for the vertical coefficients and the HH for diagonal coefficients with the numerals being the level of transform. The logo in its compressed form is added to the wavelet coefficients via a pseudorandom distribution covering all parts of the carrier image as in figure 3.

The scheme of SVD operation on the logo is based on first iterating a 32x32 logo to get a 128x128 iterated logo. This is followed by undergoing SVD operation on the square iterated logo to get the two orthogonal matrices U and V and the diagonal matrix S all of size 128x128. Then instead of using the whole set of matrix values, using the feature of SVD operation only (2x128xk+k) values are used where k is a small value compared to 128. In this scheme k=11 has been used for which only 2827 pixels are to be hidden in the carrier image.

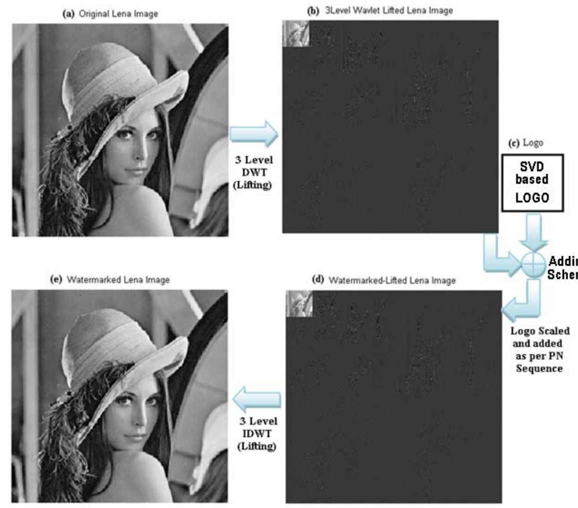

Figure 3. The watermarking process with (a) Original Image; (b) 3 Level Lifted DWT; (c) SVD based LOGO; (d) Watermarked 3 Level Lifted DWT and (e) 3 Level Lifted inverse DWT image i.e. the watermarked image.

In this method the HH1 band is left free as it contains the diagonal components of high frequency both row as well as column wise. In the rest, the U and V pixels (i.e. 1408 each) are distributed in the first horizontal and vertical coefficient sets of 128x128 (16348) values LH1 and HL1, respectively. While the main (11) diagonal components of S are multipled and distributed in the LL1 band decomposed to LL3, LH3, HL3, HH3, LH2, HL2 and HH2. All of these distributions for the U, V and multipled S are based on a particular seed ('key') used to generate the pseudorandom sequence based on which these are distributed. The scheme is in figure 4. Later the 3 level lifting based inverse discrete wavelet transform is undergone to get back the watermarked image.

B. Watermark Extraction

The detection of the watermark from the stego image is just the reverse of the embedding operation. This extraction process is of non-oblivious type. As the 'key' i.e. initial seed for the pseudorandom sequence and the value of 'k' i.e. the number of elements of the diagonal S matrix are to be known at the receiver side. This is because the stego image when received under goes the reverse process of the embedding scheme. This is as the received image is first undergone 3 level lifting based DWT followed by accumulation of the receiver end the compressed U, V and S matrix elements by the use of 'key'(seed) value to get the pseudorandom positions in the LH1, HL1 and other sub coefficients in level 2 and level 3, respectively. This collection of elements is limited by the value of 'k' which

DOI: 01.IJSIP.02.01.83

determines the number of elements in each pseudorandom distribution, to get (128xk) for U and V and multipled 'k' elements for S. The matrices once deduced are undergone the inverse SVD operation $UxSxV^T$ to get the iterated logo matrix of size 128x128. If the matrix is clear with all the iterated logos clearly visible and in binary form then it is concluded that the carrier image has not been tampered with while if any single pixel in the carrier image is altered that will be evident from the logo extracted having a low peak signal to noise ratio (PSNR) than the original compressed logo.

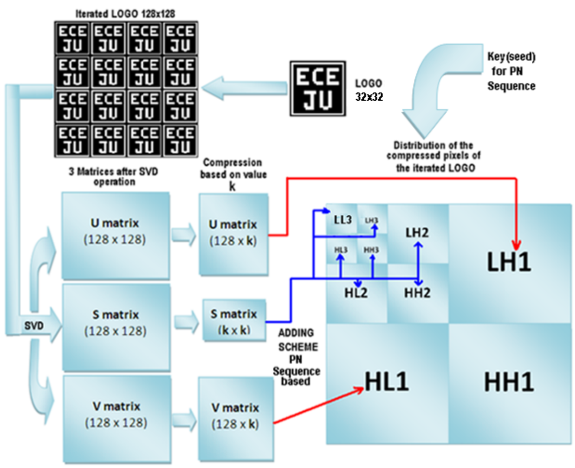

Figure 4. The encoding scheme of the compressed logo in SVD transform domain in the wavelet domain.

III. Result and Analysis

The original image when watermarked with the aforementioned scheme is with PSNR of 42.2 dB. Thus, as for good and imperceptible watermark the PSNR of 35-40dB is reasonable, so the pay load does not create problem. The original watermarked image along with the iterated logo is given in figure 5.

Figure 5. The watermarked lena image (256x256) with PSNR of 42.2dB with the original iterated logo (128x128).

Though the HH1 set of coefficients were not containing any watermark data, still if any alteration is done in the high frequency they can be detected as the other bands like LH1, HL1, HH2, LH2, HL2, HH3, LH3 and HL3 too contain a good deal of high frequency components and they are all inter related mathematically unless there is any tampering. The resultant logo alterations achieved to indicate the tampering for some of the popular attacks are provided in figures 6 to 11. The attacks considered are single row of pixel altered with a different pixel intensity, image cropping, image filtering, Gaussian noise attack with mean zero and variance of 0.02, high density of 0.2 salt and pepper noise attack and the pixel copy attack. Here the extracted logo can be identified to have the original iterated logo characteristics even after the attacks. Along with this the distribution of the attack can also be realized by observing the logo extracted and comparing with the original iterated logo.

Conclusions

This SVD and lifting based discrete wavelet transform based system of fragile watermarking fulfils its purpose of authenticating the carrier image, as observed for the attacks considered. The region of attack or tampering can be detected by viewing the alterations in the extracted logo and comparing it with the original. Unlike other popular methods of watermarking this is not a hybrid scheme, involving two transforms on the carrier itself. Rather one of the transforms act on the carrier and the other on the logo to be embedded, separately. The main key feature here of both the transforms is that, both of them can be easily implemented in hardware. This is a very important advantage, as present-day systems are more oriented for speed and miniaturization. So with the feature of easier hardware implementability, both of these are taken into account.

Figure 6. The single pixel line alteration attack, where the first row of pixel was modified and resultant effect on the logo.

Figure 7. The image crop attack and resultant effect on the logo.

DOI: 01.IJSIP.02.01.83

Figure 8. The image filtering attack and resultant effect on the logo.

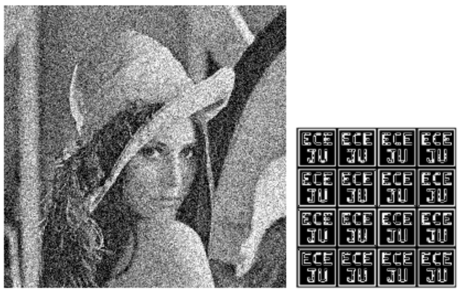

Figure 9. The Gaussian noise attack and resultant effect on the logo.

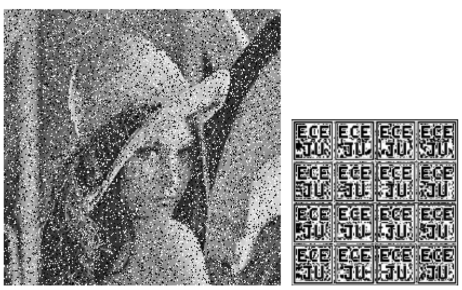

Figure 10. The salt and pepper noise attack and resultant effect on the logo.

Figure 11. The pixel alteration attack and resultant effect on the logo.

REFERENCES

[1] E. T. Lin and E. J. Delp, “A Review of Fragile Image Watermarks”, Proceedings of the Multimedia and Security Workshop, pp. 25-29, 1999.

[2] Deepa Kundur and Dimitrios Hatzinakos, “Digital Watermarking for Telltale Tamper Proofing and Authentication”, Proceedings of IEEE, Vol. 87, No.7, pp. 1167-1180, 1999.

[3] M. Swanson, M. Kobayashi, A. Tewfik, “Multimedia data-embedding and watermarking technologies,” Proceedings of the IEEE, vol. 86, no. 6, pp. 1064-1087, June 1998.

[4] D. Stinson, Cryptography Theory and Practice, CRC Press, Boca Raton, 1995.

[5] R. Wolfgang and E. Delp, “Fragile watermarking using the VW2D watermark,” Proceedings of the IS&T/SPIE Conference on Security and Watermarking of Multimedia Contents, pp. 204-213, San Jose, California, January 1999.

[6] N. Memon, S. Shende, and P. Wong, “On the security of the Yueng-Mintzer Authentication Watermark,” Final Program and Proceedings of the IS&T PICS 99, pp. 301-306, Savanna, Georgia, April 1999.

[7] R. Wolfgang and E. Delp, “A watermark for digital images,” Proceedings of the IEEE International Conference on Image Processing, vol. 3, pp. 219-222, 1996.

[8] M. Wu and B. Liu, “Watermarking for image authentication,” Proceedings of the IEEE International Conference on Image Processing, vol. 2, pp. 437-441, Chicago, Illinois, October 1998.

[9] L. Xie and G. Arce, “Joint wavelet compression and authentication watermarking,” Proceedings of the IEEE International Conference on Image Processing, vol. 2, pp. 427-431, Chicago, Illinois, October 1998.

[10] W. Sweldens. The lifting scheme: A custom-design construction of biorthogonal wavelets. Appl. Comput. Harmon. Anal., 3(2):186–200, 1996.

[11] Ruizhen Liu and Tieniu Tan, "A SVD-based watermarking scheme for protecting rightful ownership", IEEE transactions on multimedia, vol. 4, pp 121-128, March 2002

[12] Xinzhong Zhu, Jianmin Zhao and Huiying Xu, "A digital watermarking algorithm and implementation based on improved SVD" proceedings of the 18th IEEE Computer Society International Conference on Pattern Recognition (ICPR'06)

[13] S. Majumder and M. A. Hussain, “A comparative study of image compression techniques based on SVD, DWT-SVD and DWT-DCT” pg 500-504 at International Conference on Systemics, Cybernetics, Informatics (ICSCI-2008).

[14] S. Majumder, A.D. Singh, and M. Mishra, "A Hybrid SVD and Wavelet based Watermarking", pg 197-20, at 2nd National Conference Mathematical Techniques: Emerging Paradigms for Electronics and IT Industries (MATEIT 08).

[15] S. Majumder, T.S. Das, V.H. Mankar and S.K. Sarkar, "SVD and Error Control Coding based Digital Image Watermarking", International Conference on Advances in Computing, Control, and Telecommunication Technologies (ACT 2009), pg 60-63, ISBN 978-0-7695-3915-7

[16] S. Majumder, T. S. Das, S. Sarkar, S. K. Sarkar, "Image Watermarking by Fast Lifting Wavelet Transform", proceedings of 3rd National Conference Mathematical Techniques: Emerging Paradigms for Electronics and IT Industries (MATEIT '10), January 2010.

[17] S. Majumder, T.S. Das, V.H. Mankar and S.K. Sarkar, "SVD and Neural Network based Watermarking Scheme", proceedings of International Conference on Recent Trends in Business Administration and Information Processing (BAIP 2010), Springer LNCS-CCIS, ISSN: 1865-0929

DOI: 01.IJSIP.02.01.83